(1) The Federal Trade Commission (FTC) has been at the forefront of educating the public about protecting their identities. You have also put agencies on notice about eliminating the unnecessary use and display of SSNs. What trends are you seeing with respect to ID theft and the use of SSNs in those thefts? Are things getting better or worse?

In 2010, as in prior years, identity theft was the leading complaint category that the Commission received from consumers. Government documents/benefits fraud (19%) was the most common form of reported identity theft in 2010, followed by credit card fraud (15%), phone or utilities fraud (14%), and employment fraud (11%). Government documents/benefits fraud increased 4% since 2008, while identity theft-related credit card fraud declined 5% during the same period. Our complaint data does not specifically track the use of SSNs in those identity thefts. Moreover, in many instances identity theft victims cannot determine with precision the specific personal information that led to the crime. As a result, we are not able to assess trends regarding the use of SSNs specifically in identity theft.

(2) The President's Identity Theft Task Force referred to identity theft as "a problem with no single cause and no single solution" in its 2007 Strategic Plan. Please give us an update on what has improved since 2007 and what you see as the remaining challenges in preventing ID theft. Which public agencies, either Federal, State or local, expose the greatest number of Americans to ID theft and fraud by continuing to publicly use SSNs? Have you or your agency spoken with any of these agencies? Is there legislation that was recommended by the task force that has not been enacted but should be? Please provide a status report on the recommendations relating to authentication.

Since 2007, coordination among federal agencies on the issue of identity theft has vastly improved. An interagency Task Force, consisting of staff from DOJ, FTC, FBI, IRS, HHS and others meets bi-monthly to discuss emerging trends and issues. FTC staff regularly speaks with staff from these other government agencies regarding a variety of identity theft-related topics, including continued use of SSNs by government agencies. In addition, the Commission and other Task Force agencies have conducted extensive consumer and business education on identity theft prevention and recovery, and data protection. Many of the published educational materials discuss SSNs specifically. The Commission has not, however, surveyed which agencies at which levels of government have exposed the most consumer SSNs.

In its written testimony, the Commission cited two legislative recommendations to address the risks posed by the use of SSNs in the private sector – improved consumer authentication and standards to reduce the public display and transmission of SSNs. To date, neither of these recommendations has been enacted.

As to the authentication recommendations, the Commission believes that improved authentication can be achieved by encouraging or requiring all private sector business that have consumer accounts to adopt appropriate risk-based consumer authentication

systems that do not rely on an individual's SSN alone. Accordingly, the Commission recommends that Congress consider establishing national consumer authentication standards to verify that consumers are who they purport to be.

(3) K-12 schools continue to collect students' SSNs and use them as authenticators. Would you provide an update on this practice? How can we encourage school systems to stop this practice?

The Commission staff is currently examining the practice of schools using SSNs as authenticators. On July 12, 2011, the FTC and the Department of Justice's Office for Victims of Crime will host "Stolen Futures: A Forum on Child Identity Theft." (See www.ftc.gov/bcp/workshops/stolenfutures). One of the panels at the forum will focus on securing children's data in the educational system, especially in the K-12 arena. At the forum, leaders in the field will provide an update on current practices and explore ways to encourage school systems to better safeguard student information, including SSNs as authenticators and alternatives.

(4) I appreciate the work that the Federal Trade Commission has done to address the problems of ID theft, especially ID theft among children and foster children. I hope that you will continue to address these issues. In terms of ID theft among foster children, how widespread is the problem and why are foster youth particularly vulnerable to identity theft?

Foster children are particularly vulnerable to identity theft because their personal information is easily accessible by many people, including relatives, foster parents, and state employees. Moreover, since foster children often lack a strong familial or social safety net, they tend to have fewer resources to help them once they become victims. Finally, the consequences of identity theft may be more severe for foster children because once they are emancipated from foster care, establishing good credit is essential in their process to establishing a strong start to adulthood. At the upcoming forum on child identity theft, a panel will focus on these challenging issues, as well as discuss enacted and proposed state and federal legislation related to foster children and identity theft.

(5) What types of actions is the Commission taking to assist child welfare agencies in preventing ID theft and helping victimized youth recovery their identities?

The July 12th forum on child identity theft will include a panel on the issue of identity theft in the foster care context. One of the panelists, Howard Davidson of the ABA's Commission on Children and the Law, will explore what child welfare agencies can do to help prevent identity theft. We plan to work with Mr. Davidson and other panelists after the forum to continue to collaborate on foster child identity theft issues.

(6) Are there any policy recommendations that you would make to Congress to reduce the number of foster children who are victims of ID theft?

FTC staff is currently examining the issue of identity theft in the context of foster care. Although the July 12 forum is focused on developing and disseminating outreach

messages to prevent identity theft and assist victims, the Commission staff will be sure to offer any policy recommendations as appropriate.

(7) In your written testimony, you say that the Commission recommends eliminating the unnecessary display of SSNs, including on identification cards. Does the Commission recommend ending the use of the SSN as an identifier for foster children?

As explained above, this is an issue that staff will be exploring at the July 12 forum. Based upon what staff learns, policy recommendations may be provided at a later date.

(8) Do you believe that we are winning or losing the battle against ID theft?

Identity theft continues to be a significant problem, which the Commission is trying hard to address in several ways, as described in its written testimony. Commission staff believes that its robust data security enforcement program has encouraged companies to invest in better data security to avoid having consumers' information fall into the hands of identity thieves. The Commission has also worked hard to educate consumers in how to better protect themselves from identity theft. It has disseminated millions of copies of its consumer education materials. Of course, much work remains to be done, and the Commission continues to devote resources to this important issue.

(9) How has ID theft changed over the last several years? Is it more widespread, sophisticated and harder to stop? What are the trends with respect to organized crime or state sponsored ID theft?

(10) What is the most common cause of ID theft? Is it lost or stolen Social Security cards, death records that are sold with SSNs, or via some public listing or even the internet? Are there some trends you can discuss?

[Answer to questions 9 and 10] In response to question 1, we have provided information about some trends relating to consumer complaints that the FTC has received over the past several years. However, we do not want to suggest that the unverified complaints we receive are indicative of broader trends in identity theft. The number and types of complaints we receive vary with press stories about identity theft and other unrelated factors. Because the Commission has never attempted to conduct year-to-year surveys or analyses of general trends in identity theft, we cannot speak to issues such as the level of sophistication of identity thieves or what percentage of identity theft is state-sponsored.

That said, we do know that there are many causes of identity theft including high-tech (e.g., hacking, phishing, malware, spyware and keystroke logging) and low-tech causes (e.g. dumpster diving, stealing workplace records, stealing mail or wallets, and accessing public records containing SSNs). Some thieves fabricate SSNs that correspond to active SSNs that have been issued previously to individuals, especially children. Identity theft

can also occur when an individual uses someone else's personal information, including their SSN, to obtain employment, file tax returns, or obtain other government benefits.

(11) Can you tell us what burdens may occur by removing 'unnecessary' display of SSNs? Is there a way to encourage proper use of SSNs while minimizing those burdens?

The challenge in combating the misuse of SSNs is to find the proper balance between the need to keep SSNs out of the hands of identity thieves and the need to give businesses and government entities sufficient means to attribute information to the correct person. Business and governments use SSNs to ensure accurate matching of consumers with their information. SSN databases are also used to fight identity theft – for example, to confirm that a SSN provided by a loan applicant does not, in fact, belong to someone who is deceased. To encourage proper use of SSNs while minimizing burdens of removing SSNs, the Commission has identified two key legislative recommendations – improved consumer authentication and standards to reduce the public display and transmission of SSN. In terms of the second recommendation, the Commission recommends eliminating the unnecessary display of SSNs on publicly-available documents and identification cards and limiting how SSNs can be transmitted. Such steps would reduce the availability of SSNs to thieves, without hindering the use of SSNs for legitimate identification and matching purposes.

(12) One of the interesting parts of Mr. O'Carroll's testimony is the story of Dr. Martinez, which thankfully has been successfully resolved through the arrest of his ID thief. However, Dr. Martinez had yearly audits from the IRS, even through they knew after the first contact that his wages were falsely reported due to ID fraud. Are there good examples of private or public sector entities doing more to recognize what has happened to a victim and in some way "certify" his or her experience so he or she can move on with his or her life and not be repeatedly questioned about who they are?

Some states offer identity theft victims a "passport" that the victim can carry to prove who they are. The passport – which typically may be obtained through a state's Office of Attorney General – may be useful in the event that an identity theft victim is confused with an actual or suspected criminal. In addition, the Commission staff recommends that identity theft victims obtain a detailed police report that will help to prove their innocence and enable them to clear their name, especially if new accounts are opened.[1] The Commission also recommends that Congress consider creating national standards for the public display and transmission of SSNs.

---

[1] A police report, coupled with an identity theft affidavit, creates an ID Theft Report, which enables victims to exercise certain federal rights to clear their name. Among other things, an ID Theft Report enables victims to place an extended fraud alert on their credit files for seven years, to block erroneous information on their credit files, and obtain documents underlying the crime that can be used to prove their innocence.

(13) What can individuals do to protect themselves through any public or private institutions before SSN fraud starts?

To protect themselves from SSN fraud, consumers should avoid carrying their SSN in their wallets or purses. They should be wary about giving out their SSN to any public or private institution unless it is clear why that institution needs the SSN. Consumers should also regularly check their credit reports and financial statements. Consumers may get free annual credit reports from the three credit reporting agencies through www.annualcreditreport.com.

(14) What are three things that everyone can do to prevent becoming a victim of ID theft?

Although there are no iron-clad methods for preventing identity theft, everyone should: (1) check their bank statements and credit card statements monthly, and credit report at least annually; (2) secure their personal information – if it is paper, lock it and/or shred it; if it is online, use secure Internet connections and regularly update anti-virus software; and (3) not give out their personal information in person, on the phone, through the mail, or over the Internet unless they know who they are dealing with.

(15) Federal, state and local governments still display, or sometimes truncate, SSNs on public documents. To what extent does the public display of SSNs contribute to ID theft? What findings do you have on the display of SSNs by government at all levels and what are your recommendations?

As a result of the President's Task Force on Identity Theft, many federal agencies have eliminated or reduced their collection and display of SSNs. Further, OPM has issued guidelines to federal agencies on the appropriate and inappropriate use of SSNs in federal employee records. Most recently, the Department of Defense recently announced its elimination of SSNs as an identifier. As noted above, the Commission has supported legislation to minimize public display and transmission of SSNs.

(16) The latest trend in credit cards is to use smart phones to make credit card purchases. Given the recent agency and congressional concerns about data security and tracking through the phones, do you have any concerns about SSNs and credit card use by smart phones?

The Commission staff is analyzing the developments in the mobile marketplace, including how new services and technologies offered through smart phones treat personal information – such as SSNs and credit cards data. The use of mobile phones as payment mechanisms is still evolving. To address emerging issues in the mobile arena, the Commission has established a Bureau-wide team working extensively on issues related to the mobile marketplace, examining both privacy and data security issues. We have several active mobile investigations focusing on the collection of consumer data in

general and we will continue to closely watch the security of data collected by -- and through -- mobile devices.

(17) Can you give us any recommendations on how to prevent the growing ID theft problems with children and even unborn children? What should parents do to protect their children's financial record? Are there any policy changes we can make to help parents resolve ID theft issues on behalf of their children?

At the July 12th Forum, panelists from the government, the private sector, and advocacy and non-profit organizations will explore existing and potential solutions to child ID theft. The panelists specifically will explore solutions, as well as the best advice for parents to prevent and remedy child ID theft. Armed with this information, the Commission staff will be better able to advise parents on how to safeguard their children's personal information and resolve identity theft issues.